Joseph Leckie Academy

Information Governance Strategy

This policy is reviewed annually

History of Document

Approved by Trustees: September 2021
Review date for Document: September 2022

1. Introduction

1.1 The Data Protection Act 2018 and the General Data Protection Regulations (GDPR) 2016 sets out the legal requirements, which schools are obliged to follow with regard to Information Governance. This Information Governance Strategy confirms the Academy's commitments to these requirements. It also recognises students are at the heart of its business and brings together recognition of new ways of working and developing services to better meet their needs. This Information Governance Strategy also establishes a culture of individual responsibility for Information Governance, informed and supported by awareness and training for employees, Trustees and others working for or on behalf of the Academy. This will enable all to understand the importance of Information Governance, know their responsibilities, and manage information appropriately.

1.2 This Information Governance Strategy and associated policies apply to all employees, Trustees and anyone else working for or on behalf of the Academy i.e. partners, contractors and agents.

1.3 Non-compliance with this Strategy and the associated polices could potentially expose the Academy and/or it's students, parents/carers and employees to unacceptable risk. Section 8 Governance and Compliance details responsibilities and consequences for non-compliance applicable to all. To this end, the Academy commits to:

- **Information Governance Management:** establishing and supporting robust operational and management accountability structures, with appropriate resources and expertise to ensure Information Governance issues are dealt with appropriately, effectively and at levels within the organisation commensurate with the type and gravity of the issue in question.
- **Employee Empowerment:** embedding a culture of individual responsibility and capability across the Academy in relation to information management, protection and use as part of 'business as usual'.
- **Training and Awareness:** implementing a system of training and awareness that meets government and contractual mandatory requirements, is role based, assessed and capable of equipping employees with the skills and knowledge necessary to do their jobs and respond to customer demand while complying with the Data Protection Regulations and Information Security requirements.
- **Systems and Processes:** establishing and maintaining information systems and processes to enable the efficient and secure storage and retrieval of information and the management of information risk.
- **Policy and guidance:** developing and embedding, policies and guidance documents in relation to the respective areas of Information Governance that support employees to fully understand the standards, practices and responsibilities required within the Information Governance Strategy and to take appropriate action where necessary.
- **Audit:** monitoring employee compliance with the Information Governance Strategy and associated polices through regular audits and reports.

1.4 Associated Policies

The following policies are associated with the Academy's Information Governance Strategy

- Information Risk and Security
- CCTV Policy
- Data Protection Policy
- Confidentiality Policy

- Information Rights Policy
- Records Management Policy and Schedule
- Incident Management Policy

All policies can be found on the Joseph Leckie Academy website, or a hardcopy can be requested from the Academy Reception. See Appendix 1 for policy contents pages.

1.5 This Strategy and associated policies are intended to ensure that there is a robust strategy concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the Academy and ensuring that relevant and accurate information is available where and when it is needed to improve service delivery to students and parents/carers. It will also ensure that measures are in place to reduce the occurrence of breaches in information security.

1.6 This Information Governance Strategy is owned by the Information Asset Owner (IAO) and all existing procedures relating to Information Management, Information Security, Access to Information and Records Management will now fall under this policy.

This Strategy will seek to bring together all of the existing procedures, requirements, standards and best practices and review/update them as appropriate.

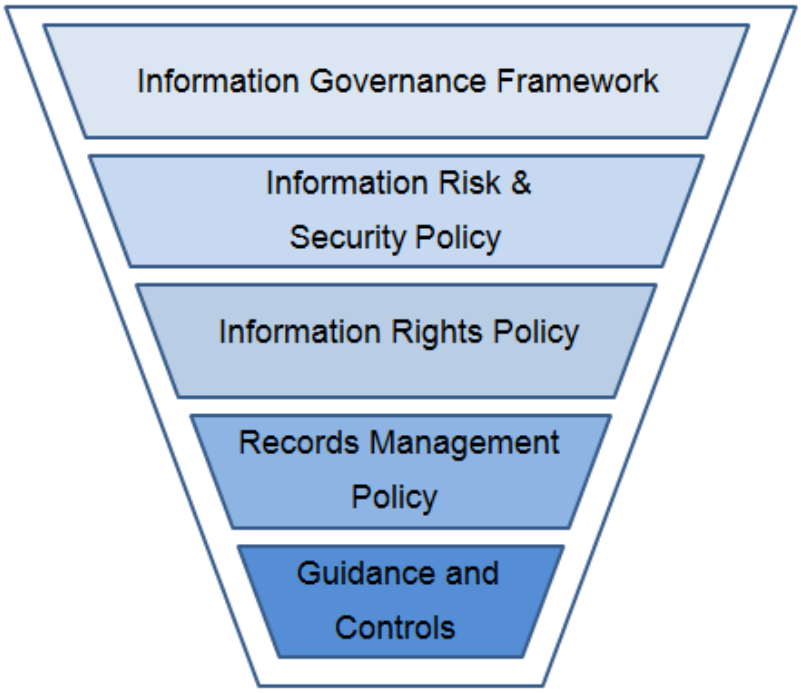

Fig 1: Information Governance Strategy

2. Purpose

2.1 The Information Governance Strategy will underpin the Academy's strategic goals and ensure that the information needed to support and deliver their implementation is reliably available, accurate and understandable.

2.2 Information within the Academy takes many forms including data stored on computers, transmitted across networks, presented on web pages, printed or written on paper, sent by fax, stored on tapes, CDs, DVDs or spoken verbally, directly or indirectly.

2.3 Information is a vital asset for the Academy, supporting both day-to-day operations and the effective management of services and resources. Information is also important in regard to improvements to service delivery and how the Academy is able to respond to changing needs and demands. Therefore, it is essential that all Academy information is managed effectively within a robust Information Governance Strategy.

2.4 Successful application of this approach will lead to:

- Affective identification, management and or mitigation of information, risks, breaches and incidents.
- Appropriate and adequate processes and awareness to support the duty of confidentiality and compliance of the data protection regulations.
- Improvements in information handling and processing activities.
- Increased customer confidence in the Academy and its employees with regards to information collection and processing.
- Supported sharing of lessons learnt and best practice.

3. What is Information Governance?

3.1 'Information Governance' describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used by the Academy are sourced, held and used appropriately, securely and legally. Information Governance ensures appropriate controls, responsibilities and actions for the security, confidentiality and protection of information is embedded into the Academy's business as usual and covers all information held by the Academy (for example – students, parents and employees, financial and corporate) and all "information systems" (assets) used to hold that information.

3.2 Systems may be purely paper-based or partially or totally electronic. The information concerned may be "owned by" or required for use by the Academy and hence may be internal or external.

3.3 As a provider of educational services, the Academy carries a responsibility for handling and protecting information of many types and categories. These types of information include personal data, commercially sensitive/confidential data and non-confidential/public data alongside business critical information.

3.4 Having accurate relevant information available at the time and place where it is needed, is critical in all areas of the Academy's business and plays a key part in corporate governance, strategic risk, service development and performance improvement and overall meeting the needs of our customers. It also supports the Academy's commitment to transparency and the Open Data agenda alongside the requirements for Privacy by Design (PbD).

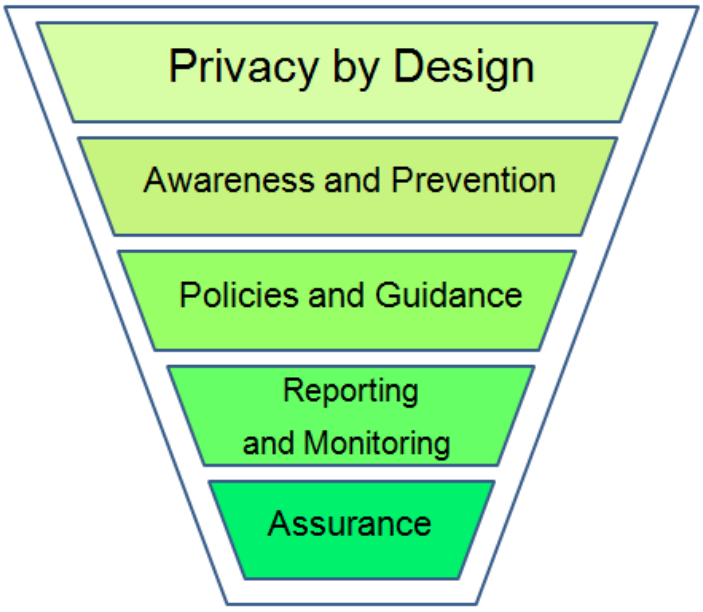

Fig 2: Privacy by Design Framework

Good Information Governance will enable the Academy to meet national and legal requirements. The Academy is obliged to abide by all relevant UK legislation

4. Applying the Strategy

4.1 In adopting this Information Governance Strategy, the Academy recognises and supports:

- The principle that accurate, timely and relevant information is a legal requirement and essential to deliver high quality services and that it is the responsibility of anyone working for or on behalf of the Academy to ensure and promote the quality of information and to actively use information in decision-making processes.
- The need for an appropriate balance between openness and confidentiality in the management and use of information.
- That the principles of corporate governance and public accountability place equal importance on the confidentiality of, and the security arrangements to safeguard, both personal information about students, parents/carers and employees and commercially sensitive information.
- The need to share information with other organisations in a controlled and secure manner consistent with the interests of the students, parents/carers and employees and, in some circumstances, the public interest.

5. Delivery

5.1 Through implementing this Strategy, the Academy will:

- Establish robust Information Governance processes conforming to statutory requirements and national standards.
- Ensure that all practices and procedures relating to collection, processing and or sharing of personal, sensitive and Academy corporate information are legal and conform to best and/or recommended practices or standards.
- Ensure that clear advice is given to students and parents about how their personal information is recorded, handled, stored and shared by the Academy and its partners. The Academy will also provide them with guidance, to explain their rights, how their personal

information is handled, how they can seek further information and how they can raise concerns.

- Ensure appropriate levels of security are applied at all times, e.g. Through the use of data protection impact assessments (DPIA) and or information security assessments.
- Provide clear advice and guidance to employees and ensure that they understand their responsibilities and apply the principles of Information Governance to their working practice in relation to protecting the confidentiality and security of personal information and appropriate handling and maintenance of academy information assets.
- Maintain a clear reporting structure and ensure through management action and training that all individuals working for or on behalf of the Academy understand Information Governance requirements alongside the duties of confidentiality and data protection.
- Undertake reviews and audits of how information is recorded, held and used. Management audits will be used to identify good practice and opportunities for improvement alongside the mitigation of identifiable risks.
- Ensure procedures are reviewed to monitor their effectiveness so that improvements or deterioration in information handling standards can be recognised and addressed
- Ensure that when service developments or modifications are undertaken, a review is undertaken of all aspects of Information Governance arrangements to ensure that they are robust and effective
- Work to instil an Information Governance culture in the Academy through increasing awareness and providing training on the key issues
- Ensure there are robust procedures for notifying and learning from Information Governance breaches and security incidents in line with the Academy's Information Risk and Security Policy, which forms part of this Strategy.
- Ensure all employees undertake the appropriate level of Information Governance awareness training for their role on an annual basis. The requirement of any further information risk and security or records management training will be subject to the role of the individual.

5.2 There are five interlinked principles, which guide the application of this Information Governance Strategy:

- Quality Assurance
- Legal Compliance
- Information Security
- Proactive use of information
- Openness and transparency

5.3 To ensure Information **Quality Assurance**, the Academy will:

- Establish, maintain and promote policies and procedures for information quality assurance and the effective management of records.
- Undertake or commission assessments and audits of its information quality and records management arrangements.
- Ensure that key student, parent/carer and employee data is accurately recorded and maintained, including regular cross-checking against source data.
- Ensure that managers as information asset owners (IAOS) are required to take ownership of, and seek to improve the quality of information within their services and that information quality is assured at the point of collection.

- Ensure that appropriate reports and records are maintained in line with the requirements to capture and assess processing activities.

5.4 To ensure **Legal Compliance,** the Academy will:

- Regard all identifiable personal information relating to students, parents and employees as confidential except where national requirements on accountability and openness require otherwise.
- Establish and maintain policies or procedures to ensure compliance with relevant law and regulation including the Data Protection Act 2018, the GDPR 2016, the human rights act, the common law duty of confidentiality and all associated guidance.
- Establish and maintain policies or procedures for the controlled and appropriate sharing of information with other agencies, taking account of relevant legislation (e.g. Health and social care act, crime and disorder act, protection of children act) or any other requirements for data sharing in accordance with national contracts and or public tasks.

5.5 To ensure that appropriate and legal compliant **Information Security** exists, the Academy will:

- Establish and maintain an Information Risk & Security Policy along with respective procedures for effective policing and secure management of all its Information Assets, resources and IT systems.
- Undertake and/or commission assessments and audits of its information and IT security arrangements in line with the said policy.
- Promote effective confidentiality and security practices to ensure all permanent/temporary, contracted employees and third party associates of the Academy adhere to this via appropriate laid down policy procedures, training and information awareness schemes/documentation.
- Establish and maintain appropriate policing, incident reporting procedures and monitoring and investigations of all instances, actual and/or potential, along with any reported breaches of confidentiality, security or the Data Protection Act 2018 and the GDPR 2016 Protection Principles.
- Identify and classify information to ensure that it is handled and shared appropriately.
- Ensure effective reports, processes and records are in place to provide information asset owners with the ability to identify risks and take actions.

5.6 To ensure **Proactive use of Information**, the Academy will:

- Ensure the Academy embeds and monitors data protection by design by proactively assessing changes to the way we create, use, store and or share information.
- Ensure systems are in place to recognise information assets and owners.
- Ensure systems and or processes are in place to recognise, identify and take action against information risks.
- Ensure information systems hold the information required to support student, parent/carer and employee focused service delivery and operational management.
- Develop information systems and reporting processes which support effective performance management and monitoring.
- Develop information management awareness and training programmes to support managers in using information to manage and develop services.

- Ensure that, where appropriate and subject to confidentiality constraints, information is shared with other organisations in order to support improved service delivery.

5.7 To ensure **Openness**, the Academy will:

- Ensure that non-confidential information about the Academy and its services is readily and easily available through a variety of media, in line with the Academy's Freedom of Information (FOI) Publication Scheme.
- Implement policies to ensure compliance with the Freedom of Information Act and the Environmental Information Regulations (EIR).
- Ensure that students, parents/carers and employees have readily and easily available access to information relating to Academy services, and their rights as service users.
- Have clear procedures and arrangements for liaison with the press and broadcasting media.
- Ensure appropriate Privacy Notices are in place to capture the requirements of the GDPR 2016 in providing data subjects with adequate and appropriate information over the way in which the Academy collects processes and shares information while ensuring the rights of individuals are clearly identified.

6. Information Governance Roles and Responsibilities

6.1 The Information Governance Structure in the Academy consists of the following:

Information Asset owner	Mr James Ludlow
Data Protection Officer	Paul Withers
External Schools Lead	Sohila Bibi
Data Protection Lead	Cassie Stroud
Board of Trustees	

7. Strategic Implementation

7.1 The Academy will monitor implementation of this Strategy through regular meetings with board of Trustees, which will involve:

- Ensuring the development and review of policies and procedures required for Information Governance and having final approval of these documents.
- Ensuring appropriate resources are in place to achieve compliance of the regulatory requirements.
- Reporting on progress, incidents and issues to Board of Trustees.

7.2 This Strategy will be reviewed annually or as required in response to any significant legislative changes, mandatory requirements, national guidance or as a result of significant Information Governance breaches or incidents and approved by the information Asset Owner and Board of Trustees.

7.3 The Information Asset Owner will be a key part of this process as they are the officer accountable for information assets across the Academy and are responsible for ensuring that appropriate Information Governance arrangements are in place locally and that national or legal requirements are met.

8. Governance and Compliance

8.1 Non-compliance with this Strategy and associated policies could potentially expose the Academy and/or its service users to risk. The potential impact of damage or loss of information

includes disruption to services, risk to citizens, damage to reputation, legal action, personal distress, loss of confidence, or media coverage and may take considerable time and cost to recover.

8.2 **Employees.** All new employees will receive awareness training and guidance on Information Governance, which will include:

- Confidentiality
- Data Protection
- Information and Cyber Security
- Information Rights

All employees will be required to repeat their Information Governance (Data Protection) awareness training annually between September and October.

Employees who do not comply with these policies/procedures may therefore be subject to disciplinary action, in line with the Academy's disciplinary procedures.

8.3 **Board of Trustees**. All Trustees will also receive annual awareness training and guidance on Information Governance, which will include confidentiality, data protection, information security and cyber security alongside lessons learnt and proactive data security notices. Members' failure to comply with these policies/procedures will constitute a potential breach of the Academy's Code of Conduct.

8.3 **Others Working on Behalf of the Academy**. Any persons working for and on behalf of the Academy must undertake appropriate awareness training prior to gaining access to Academy held information or business critical data/systems. All managers are therefore responsible for ensuring that any person, agent, consultant, temporary or honorary employee must comply with national, legal and local Information Governance awareness and abide by the duties of confidentiality and data protection.

8.4 Responsibilities

8.4.1 The Principal shall have overall responsibility for managing and implementing the Strategy and associated policies and procedures on a day-to-day basis.

8.4.2 Managers are responsible for ensuring that their permanent and temporary employees and contractors have:

- read and understood this Strategy and the associated policies and procedures applicable in their work areas.
- been made aware of their personal responsibilities and duties in relation to Information Governance.
- been made aware of who to contact for further advice.
- Received appropriate and up-to-date training relating to Information Governance.
- Abide by the Academy's Code of Conduct.

8.4.3 The following table identifies who within the Academy is Accountable, Responsible, Informed or Consulted with regards to this Strategy. The following definitions apply:

- **Accountable:** the person who has ultimate accountability and authority for the Strategy.

- **Responsible:** the person(s) responsible for developing and implementing and reviewing the Strategy.
- **Consulted:** the person(s) or groups to be consulted when the Strategy is reviewed and approved
- **Informed:** the person(s) or groups to be informed throughout the approval process.

Accountable	Senior Information Risk Owner (Principal)
Responsible	Data Protection Officer / Data Protection Lead
Consulted	Board of Trustees
Informed	All individuals employed by the Academy either permanently, on a temporary basis or as a contractor, and partner organisations.

9. Non-Compliance

Non-compliance with this Strategy or associated policies/procedures/guidance may therefore be subject to disciplinary action, in line with the Academy's disciplinary procedures and or legal action if appropriate.

10. Definitions

Term	Definition
Personal data	The General Data Protection Regulation (GDPR) 2016 only applies to organisations' use of personal data. This is any information relating to an identified, or identifiable, person. This may include information such as the person's: • Name • Contact details • Identification number • Online identifier, such as a username It may also include anything relating to the person's physical and mental health, genetics, finances, or their physiological, cultural, or social identity.
Special categories of personal data	Personal data which is considered to be more sensitive and therefore requires further safeguards: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Trade union membership • Genetic data • Biometric data where used for identification purposes (such as fingerprints, retina and iris patterns) • Health – physical or mental • Sex life or sexual orientation

	• Criminal offences and procedures
Processing	Anything operation or set of operations performed on personal data including: collecting, recording, organising, structuring, storing, adapting, altering, retrieving, using, disseminating, erasing or destroying. Processing can be automated or manual.
Data Subject	The identified or identifiable individual to whom the personal data relates (e.g. all your students, parents/carers, employees will be data subjects).
Data Controller	A person or organisation that determines the purposes and means of processing of personal data (e.g. you as an Academy)
Data Processor	An external person or organisation, who is **not** employed by your Academy, who processes the personal data on your Academy's behalf (e.g. your payroll provider, an external careers advice service, or your parental communications provider).
Data Protection Officer	The person in your Academy, or an external data protection adviser, who takes responsibility for monitoring data protection compliance.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, un-authorised disclosure of, or access to personal data.

11. Further Information and Associated Policies

11.1 For further information about Information Governance please visit the ICO website www.ico.org.uk

11.2 This policy should be read alongside:

- Information Risk and Security Policy
- CCTV Policy
- Data Protection Policy
- Confidentiality Policy
- Freedom of Information Policy
- Information Rights Policy
- Records Management Policy and Schedule
- Incident Management Policy
- Subject Access Request Policy
- Consent to Use Personal Data Guidance
- Impact Levels and Protective Marking Guidance

Appendix 1: Policy Contents Pages

Information Risk and Security Policy

CCTV Policy

Data Protection Policy

7. Subject Access Requests (SAR)
8. Amendments to Inaccurate Records
9. Objections to Processing
10. Releasing personal information to prevent or detect crime
11. Sharing Personal Data with Third Parties
12. Photographs and Video
13. Data Disposal
14. Complaints
16. Further Information and Associated Policies

Confidentiality Policy

1. Introduction
2. Scope
3. Legal Framework
4. Definitions
5. Policy Application
6. Limits of Confidentiality
7. Classroom Confidentiality
8. One to One Disclosures
9. Disclosures to Health Professionals
10. Breaking Confidentiality
11.Guidance for Academy
12. External Visitors
13. Informing Parents/Carers
14. Dissemination
15. Further Information and Linked Policies

Information Request Policy

1. The Academy will comply with
2. Data Gathering and Storage
3. Publication Scheme
4. Making a request
5. Dealing with Requests for Information
6. Applying Exemptions
7. Paying for information
8. Logging Requests Received
9. Further Information and Linked Policies

Information Rights Policy

1. Introduction
2. Scope
3. Freedom of Information (FOI)
4. Environmental Information Regulations (EIR)
5. Responding to FOI and EIR
6. Data Gathering and Storage
7. Publication Scheme
8. Dealing with Requests for Information

9. Applying Exemptions
10. Logging Requests Received
11. Further Information and Linked Policies

Records Management Policy and Schedule

1. Introduction
2. Purpose of Disposal Schedule
3. Closing a file
4. Minimum Retention Period
5. Destroy
6. Commitment to preserving files/records
7. Roles and Responsibilities
8. Definitions of Records held by Joseph Leckie Academy in respect of its Functional Areas.
9. Electronic Records
10. Academy Disposal Schedule
11. Further Information and Associated Policies

Incident Management Policy

1. Introduction
2. Purpose
3. Scope
4. Objectives
5. Legal Requirements
6. Compliance
7. Definition
8. Procedure for Personal Data Breach Incident Handling
9. Investigation and Report
10. Report
11. Review and Planning
12. Further Information and Associated Policies